The submitted reference was prepared by a foreign Patent Office, and is directed to a foreign counterpart application to the present US Patent Application. Consistent with Applicant's duty of disclosure under 37 CFR 1.56, Applicant recognizes that the Examiner may consider it relevant when making a patentability determination. However, this submission should not be misconstrued as an admission by the Applicant that the reference is either relevant or not relevant to patentability, especially since the reference was prepared by a foreign Patent Office that is governed by a different body of law than the USPTO.

Nevertheless, in the interest of full disclosure and good faith, Applicant submits the reference for consideration by the Examiner, and requests that the Examiner initial the attached Form PTO 1449, indicating the Examiner has considered this reference.

P.1
Notification of Reasons for Refusal

Patent application number	Japanese Patent Application No. 2002-273601
Drafting date	October 4, 2007
Examiner	Shigenori Aoki 4229 5S00
Representative of the applicant	Takahisa Sato
Applicable articles	Article 29 Paragraph 2, Article 36

This application should be refused according to the following reasons. If any arguments on these reasons for refusal exist, please file an argument within 60 days from the sending date of this notification.

Reason

(1) For this application, the description of the claims does not satisfy the requirements prescribed in Patent Law Article 36 Paragraph 6 Item 2 in the following point.
(2) Because the invention relating to the following claims in this application is an invention which could easily have been made, prior to the filing of the patent application, by a person with common knowledge in the art to which the invention pertains, on the basis of an invention described in the following publications distributed in Japan or foreign countries prior to the filling of the patent application, or on the basis of an invention which could be utilized by the publics through the telecommunication lines, the right to the patent shall not be granted in accordance with the provision of the article 29, paragraph 2 of the Patent Law.

Note (Please refer to the list of references for cited references)

About Reason (1)
(a) With regard to the description that "authentication means having key data ... supplies the first data for authentication that the means to be authenticated uses for the authentication to the means to be authenticated" in a matter described in claim 1, 13, 15 of this application can be read as not only a supplying origin and a supplying

target is the same "means to be authenticated" but also a supplying origin is the "authentication means" and a supplying target is the "means to be authenticated". Accordingly, because the subject matter in the process for "supplying" cannot be decided as single meaning so that it is unclear, the inventions concerning claim 1, 3, 15 do not satisfy the requirement prescribed in Patent Law Article 36 Paragraph 6 Item 2.

Also, with regard to the inventions concerning 2 - 12, 14, those are depending from claim 1, 13, those do not satisfy the requirement prescribed in Patent Law Article 36 Paragraph 6 Item 2 either by the similar reason.

P.2

(b) With regard to the description that "... the first data for authentication which makes the recovery of the key data difficult is generated based on the predetermined generation technique..." in a matter described in claim 1, 13, 15 of this application, it cannot be decided as single meaning whether "key data" is generated or "the first data for authentication" is generated. Accordingly, the inventions concerning claim 1,3, 15 of this application do not satisfy the requirement prescribed in Patent Law Article 36 Paragraph 6 Item 2.

Also, with regard to the inventions concerning 2 - 12, 14, those are depending from claim 1, 13, those do not satisfy the requirement prescribed in Patent Law Article 36 Paragraph 6 Item 2 either by the similar reason.

(c) With regard to "the first data for authentication" in a matter described in claim 1, 13, 15 of this application, the expression that "the first data for authentication which makes the recovery of the key data difficult" is disclosed for the first process, the first procedure, or the first means, and it can be thought that it differs from the "the first data for authentication" described previously in the point that it is difficult to recover the key data". On the other hand, because it was referred to, it can be thought that "the first data for authentication" and "the first data for authentication that makes the recovery of the key data difficult" have the same characteristics. Accordingly, the characteristics of each of the first data for authentication cannot be decided as single meaning so that the inventions concerning claim 1,3, 15 of this application do not satisfy the requirement prescribed in Patent Law Article 36 Paragraph 6 Item 2.

Also, with regard to the inventions concerning 2 - 12, 14, those are depending from claim 1, 13, those do not satisfy the requirement prescribed in Patent Law Article 36 Paragraph 6 Item 2 either by the similar reason.

(d) Although it is described in claim 4 of this application that "data for authentication generated by using the first key data relating to the processing that the first user allowed to the means to be authenticated in the first process... ", "what kind of processing done by the means to be authenticated "the processing" designates cannot be decided in single meaning so that it is unclear. Accordingly, the inventions concerning claim 4 of this application does not satisfy the requirement prescribed in Patent Law Article 36 Paragraph 6 Item 2.

Also, with regard to the inventions concerning claim 5, which is depending from claim 4 it does not satisfy the requirement prescribed in Patent Law Article 36 Paragraph 6 Item 2 either by the similar reason.

About Reason (2)

Claim: 1, 9 - 11
Cited references: 1
Remarks
A data processing method is described in cited reference 1 in which an IC card having encryption keys corresponding to plural areas generates a degeneration key based on a degeneration key generation processing according to the degeneration processing order designated by using a encryption key based on the provider number and the number of providers in an area to be accessed, the area is designated by a controller having the degeneration key generated by the degeneration processing by using an encryption key for the area to be accessed, the mutual authentication with the controller is performed by using the degeneration key of the IC card, and in the condition the it is verified that the degeneration key of the controller and degeneration key of the IC card are the same degeneration key, Read-Out and Write for the area relating to the encryption key are performed.

P.3

Also, "this degeneration key is used only for authentication so that it is not necessary to be able to decrypt the original plural encryption keys from the degeneration key" is described in paragraph [0071] of cited reference 1. Accordingly, it is disclosed that it is difficult to decrypt the encryption key in the degeneration processing performed in the IC card or the controller so that it can be done easily by a person skilled in the art to make the invention concerning claim 1 of this application functionally based on the invention described in cited reference 1.

Claim: 2
References cited: 1
Remarks
With regard to the data processing method described in cited reference 1, it shows to memorize the degeneration key generated in a memory of the controller and degeneration order especially in paragraph [0080] – [0082]. Also, it is well known to a person skilled in the art to integrate a circuit for processing, such as for the degeneration processing with a memory.

Claim: 3
References cited: 1
Remarks
With regard to the data processing method described in cited reference 1, the degeneration keys are generated by using the encryption keys relating to the processing for read-out, write from and to the area provided in the IC card and allowed by the controller.

Claim: 4, 6, 7
References cited: 1
Remarks
With regard to the degeneration processing of the data processing method described in cited reference 1, especially as shown in Fig. 3, the degeneration key is generated by a series of multiplex encryption with each encryption key corresponding to each area, respectively.

Claim: 5

References cited: 1, 2
Remarks
Because it is described in cited reference 2 to prevent a compression data from manipulation by giving the decoding using RSA method, it is a well-known art before this application.

P.4

And, with regard to the degeneration processing of the data processing method described in cited reference 1, especially as shown in Fig. 3, the degeneration key is generated by a series of multiplex encryption with each encryption key corresponding to each area, respectively. However, it can be done easily by a person skilled in the art to add a manipulation prevention function by employing the well-known art to the degeneration key and giving the decoding using RSA method.

Claim: 8
References cited: 1
Remarks
With regard to the data processing method described in cited reference, especially paragraph [0097], [0080], and Fig. 9- 11, it shows that the degeneration key of a controller is generated by using one encryption key relating to plural providers.

Claim: 12
References cited: 1, 3
Remarks
It is described in cited reference 3 (especially column 5 line 21 – 30) to provide a device in which authentication processing is executed with a display in order to check the operation or display a command and data so that it is a well-known art before the application.

Claim: 13, 14
References cited: 1
Remarks
The data processing method shown in the remarks of the claim: 1 is described in cited reference 1. It is usual practice for a person skilled in the art to be programmed to carry out the method with a data processing device.

Claim: 15
References cited: 1
Remarks
The data processing method shown in the remarks of the claim: 1 is described in cited reference 1. It is usual practice for a person skilled in the art to comprise a data processing device to carry out the method.

If any reason for refusal is found later, it will be notified.

List of cited references
1. Published patent application No. HEI 10-327142
2. Published patent application No. SHO 60-26387

P.5

3. Published patent application No. HEI 9-114946

Record of the result of the prior art reference searched

Searched Field IPC H04L9/00
Prior art document Published patent application No. HEI 11-163853

The record of the result of prior art reference searched is not the reason for refusal.

Director/Deputy
Primary examiner/Deputy Shoji Ishikawa 8524
Examiner Shigenori Aoki 4229
Assistant Examiner

拒絶理由通知書

特許出願の番号	特願２００２－２７３６０１
起案日	平成１９年１０月　４日
特許庁審査官	青木　重徳　　４２２９　５Ｓ００
特許出願人代理人	佐藤　隆久　様
適用条文	第２９条第２項、第３６条

この出願は、次の理由によって拒絶をすべきものです。これについて意見がありましたら、この通知書の発送の日から６０日以内に意見書を提出してください。

理　由

（１）この出願は、特許請求の範囲の記載が下記の点で、特許法第３６条第６項第２号に規定する要件を満たしていない。
（２）この出願の下記の請求項に係る発明は、その出願前に日本国内又は外国において、頒布された下記の刊行物に記載された発明又は電気通信回線を通じて公衆に利用可能となった発明に基いて、その出願前にその発明の属する技術の分野における通常の知識を有する者が容易に発明をすることができたものであるから、特許法第２９条第２項の規定により特許を受けることができない。

記　　（引用文献等については引用文献等一覧参照）

理由（１）について
（ａ）本願特許請求の範囲の請求項１，１３，１５に記載されている事項における、「鍵データを保持する認証手段が、…（中略）…前記被認証手段が前記認証に用いる前記第１の認証用データを前記被認証手段に提供する…（後略）…」との記載は、提供元と提供先が同じ「被認証手段」となっているとも、提供元が「認証手段」であって提供先が「被認証手段」であるとも読めることから、「提供する」処理における当事者が一義的に決定できず不明であるので、本願請求項１，３，１５に係る発明は、特許法第３６条第６項第２号に規定する要件を満たしていない。
　また、同請求項１，１３を引用する請求項２－１２，１４に係る発明についても、同様の理由により特許法第３６条第６項第２号に規定する要件を満たしていない。

（ｂ）本願特許請求の範囲の請求項１，１３，１５に記載されている事項におけ

る、「…（前略）…前記鍵データを復元困難な前記第１の認証用データを前記所定の生成手法を元に生成する…（後略）…」との記載について、「鍵データを」生成するのか、「第１の認証用データを」生成するのか、一義的に決定できず、不明であるので、本願請求項１，３，１５に係る発明は、特許法第３６条第６項第２号に規定する要件を満たしていない。
　また、同請求項１，１３を引用する請求項２－１２，１４に係る発明についても、同様の理由により特許法第３６条第６項第２号に規定する要件を満たしていない。

（ｃ）本願特許請求の範囲の請求項１，１３，１５に記載されている事項における「第１の認証用データ」について、第１の工程、あるいは第１の手順、第１の手段においては「鍵データを復元困難な前記第１の認証用データ」と表現されたものが開示されており、それ以前に記載された「第１の認証用データ」とは鍵データを復元困難な点において相違するものと考えられるが、一方で「前記」として引用したために、「第１の認証用データ」と「鍵データを復元困難な前記第１の認証用データ」が同じ特性を有するデータとも考えられ、それぞれの認証用データの特性が一義的に決定できないので、本願請求項１，３，１５に係る発明は、特許法第３６条第６項第２号に規定する要件を満たしていない。
　また、同請求項１，１３を引用する請求項２－１２，１４に係る発明について

ない。

（ｄ）本願特許請求の範囲の請求項４には「前記第１の工程において、第１のユーザが前記被認証手段に許可した前記処理に関連付けられた第１の鍵データを用いて生成した認証用データを、…（後略）…」と記載されているが、「前記処理」が被認証手段が行うどのような処理を指しているのか、一義的に決定できず不明であるから、本願請求項４に係る発明は特許法第３６条第６項第２号に規定する要件を満たしていない。
　また、同請求項４を引用する請求項５に係る発明についても、同様の理由により特許法第３６条第６項第２号に規定する要件を満たしていない。

理由（２）について
・請　求　項：１，９－１１
・引用文献等：１
・備　　考
　引用文献１には、複数のエリアに対応するそれぞれの暗号鍵を保持するＩＣカードが、アクセスすべきエリアの暗号鍵を用いて縮退処理により生成した縮退鍵を保持するコントローラから指定されたアクセスすべきエリアのプロバイダ番号とプロバイダ数に基づく暗号鍵を用いて、指定された縮退処理順序に応じた縮退鍵生成処理により縮退鍵を生成し、前記ＩＣカードの縮退鍵を用いて前記コントローラと相互認証を行い、当該相互認証により、前記コントローラの縮退鍵と前記ＩＣカードの縮退鍵とが同一の縮退鍵であることを確認したことを条件に、前記暗号鍵に関連付けられたエリアに対する読み出し、書き込みを行うデータ処理方法が記載されている。
　また、引用文献１には、段落【００７１】に「この縮退鍵は、認証に用いるだけなので、その縮退鍵から元の複数の暗号鍵を復元することが可能である必要はない。」と記載しており、前記ＩＣカードや前記コントローラにおいてなされる前記縮退処理では前記暗号鍵を復元困難とすることが開示されていることから、引用文献１に記載されている発明から、本願請求項１に係る発明を機能構成することは当業者にとって容易になし得たことである。

・請　求　項：２
・引用文献等：１
・備　　考
　引用文献１に記載されているデータ処理方法では、特に段落【００８０】－【００８２】において、コントローラのメモリに生成した縮退鍵や縮退の順序を記憶させておくことが示されているし、縮退処理といった演算処理を行う回路をメモリを含めて集積化することは、当業者にとって周知技術である。

・請　求　項：３
・引用文献等：１
・備　　考
　引用文献１に記載されているデータ処理方法では、前記コントローラに許可された前記ＩＣカードが保持するエリアへの読み出し、書き込み処理に関連付けられた前記暗号鍵を用いて前記コントローラの縮退鍵を生成している。

・請　求　項：４，６，７
・引用文献等：１
・備　　考
　引用文献１に記載されているデータ処理方法における縮退処理では、特に【図３】に示すように、各エリアに対応するそれぞれの暗号鍵によって直列多重に暗号化が実施されることで縮退鍵を生成している。

・請　求　項：５
・引用文献等：１，２
・備　　考
　圧縮したデータに対し、ＲＳＡ法により復号化を施すことで改竄防止を図ることは引用文献２に記載されており、本出願前において周知技術である。

そして、引用文献１に記載されているデータ処理方法における縮退処理では、特に【図３】に示すように、各エリアに対応するそれぞれの暗号鍵によって直列多重に暗号化が実施されることで縮退鍵を生成しているが、該縮退鍵に対して前記周知技術を採用し、ＲＳＡ法により復号化を施すことで改竄防止機能を付加することは、当業者が容易になし得たことである。

・請　求　項：８
・引用文献等：１
・備　　考
引用文献１に記載されているデータ処理方法では、特に段落【００７９】，【００８０】及び図９－１１において、複数のプロバイダに関連付けられた一つの暗号鍵を用いてコントローラの縮退鍵を生成することが示されている。

・請　求　項：１２
・引用文献等：１，３
・備　　考
動作確認やコマンドやデータの表示が行えるよう、認証処理が実行される装置にディスプレイを設けることは、引用文献３（特に第５欄第２１－３０行）に記載されており、本出願前において周知技術である。

・請　求　項：１３，１４
・引用文献等：１
・備　　考
引用文献１には上記請求項：１の備考で示すデータ処理方法が記載されているが、当該方法をデータ処理装置で実行するためにプログラム化することは、当業者にとって常套手段である。

・請　求　項：１５
・引用文献等：１
・備　　考
引用文献１には上記請求項：１の備考で示すデータ処理方法が記載されているが、当該方法を実行するためのデータ処理装置を構成することは、当業者にとって常套手段である。

拒絶の理由が新たに発見された場合には拒絶の理由が通知される。

引　用　文　献　等　一　覧
１．特開平１０－３２７１４２号公報
２．特開昭６０－２６３８７号公報

３．特開平９－１１４９４６号公報

先行技術文献調査結果の記録

・調査した分野　　ＩＰＣ　Ｈ０４Ｌ９／００
・先行技術文献　　特開平１１－１６３８５３号公報
この先行技術文献調査結果の記録は拒絶理由を構成するものではありません。

部長／代理	審査長／代理	審査官	審査官補
	石川　正二	青木　重徳	
	８５２４	４２２９	